State of Illinois
Electronic Disease Surveillance System (EDSS)
Request for Proposal
Due October 8, 2020 not later than 5:00 P.M. CST

Background

The State of Illinois is soliciting proposals to replace Illinois' National Electronic Disease Surveillance System (I-NEDSS) system, a web-based application available to health care providers, Local Health Departments and other reporters for input of demographic, medical and exposure information on patients diagnosed with reportable conditions. The State of Illinois is soliciting these proposals to secure the replacement of I-NEDSS for an emergency procurement under the Gubernatorial Disaster Proclamation due to the spread of the Coronavirus Disease (COVID-19). The State will evaluate the proposals received by the above deadline and select one Electronic Disease Surveillance System (EDSS) to replace I-NEDSS.

This request for proposal is predicated upon the State of Illinois' goal to provide a reliable state-wide disease surveillance and reporting system that can handle the increased workload created by the COVID-19 outbreak, namely millions of test results and contact traces. All proposals shall be for a permanent installation of an EDSS and shall be capable of providing surveillance for communicable and infectious diseases other than COVID-19. The proposal shall be for a full system replacement as the State of Illinois will discontinue use of the I-NEDSS system after successful transition to the new EDSS.

Key Dates

September 10:	Request for Proposal issued
September 18:	All questions from vendors due not later than 5:00 P.M. CST and submitted via email to Sean.M.McAuliff@Illinois.gov
September 25:	Answers to all vendor questions released on http://www.dph.illinois.gov/rfp/edss-rfp
October 8:	Proposal submission deadline not later than 5:00 P.M, CST via email to Sean.M.McAuliff@Illinois.gov
October 20 (estimated):	Vendor selected and engaged
November 2:	Implementation initiation

Directions

Vendors shall submit proposals for an EDSS to Sean.M.McAuliff@Illinois.gov not later than 5:00 P.M. CST on October 8, 2020. All vendors who are deemed to have submitted responsive proposals will be asked to provide a 90-minute live demonstration to the Evaluation Committee.

Each proposal submission shall include the following items:

1) Name of company submitting the proposal.

2) Point of contact name, title, phone number and email address.
3) EDSS description and explanation of how the EDSS satisfies the scope of work below.
4) Timeline for EDSS Implementation.
5) Cost for set up, implementation, training, and ongoing Software as a Service Subscription for Application and Hosting. Note – The costs must be recorded on Attachment A – Budget Template and must be attached as a separate response document.

VENDOR'S PROPOSED SOLUTION TO MEET THE STATE'S REQUIREMENTS: Please either respond in the space below or in the following prescribed format:

Mandatory Requirements

The State of Illinois is seeking the emergency procurement under the COVID-19 Gubernatorial Disaster Declaration for an Electronic Disease Surveillance System (EDSS) that will be a patient-centric model that allows all public health events for a patient to be viewed from one central location and will include:

System

M1. User-customizable decision support functionality for automated processing of Electronic Lab Reporting (ELR) and electronically-received public health case reports.

M2. Disease data entry directly through an Internet browser-based system, thereby creating a database accessible by health investigators and public health professionals.

M3. Data Warehouse capabilities for a unified repository used to report and analyze information using a common data model.

M4. Manage all reportable conditions including HIV, Sexually Transmitted Diseases, tuberculosis (TB) and all other reportable infectious diseases.

M5. Implement all Message Mapping Guides for the Centers for Disease Control and Prevention (CDC) with the ability to code values within the export integration feature of the application.

M6. TB module conforms to the 2020 Report of Verified Case of TB (RVCT).

M7. Replicate existing extended reports sent to CDC for the following conditions: Anaplasma, Brucella, Cyclospora, H. Flu, Legionella, Listeria, Lyme, Malaria, Measles, Mumps, Pertussis, Q fever, Spotted fever rickettsioses, Tularemia, Typhoid and Paratyphi A, Varicella (XML file), Vibrio, Tuberculosis (XML file).

M8. Robust rules engine and the ability to sequester lab reports and electronic case reports based on combinations of Logical Observation Identifiers Names and Codes (LOINC), Systematized Nomenclature of Medicine (SNOMED), quantitative results, and age or year of birth of case.

M9. Capability of managing all standard codes (ICD-10, SNOMED, LOINC, RxNorm) and linking the codes to reportable conditions in lookup tables within the application.

M10. Ability to support local or custom code systems for LOINCs and SNOMEDs. e.g. Illinois Department of Public Health (IDPH) code system specimen source look up (HL7-0070, HL7-0487, etc).

M11. Capability of managing reporting organizations and reporting Clinical Laboratory Improvement Amendments (CLIAs/laboratories) lookup tables within the application.

M12. Allows for custom code changes for disease case definition assignment or case auto closure.

M13. System must have capability for outbreak management.

M14. System must have capability for a job scheduler (Quartz) process schedules.

M15. System must have a robust rules engine for validation, and closure rules with regards to case investigation.

M16. Ability to upload and store historical case and outbreak data within reporting system database.

M17. System must have the ability to include an animal rabies testing module**.**

M18. System must include all diseases on the list of Illinois Reportable Diseases (https://www.dph.illinois.gov/sites/default/files/publications/illinois-stop-and-report-disease-poster.pdf) and CDC Reportable diseases (https://wwwn.cdc.gov/nndss/conditions/).

M19. The Vendor must be incorporated as a business in any state for at least three (3) years.

M20. The Vendor must have at least three (3) years' experience in developing systems comparable to this proposal in terms of functionality.

M21. The system must be a commercial off-the-shelf (COTS) system.

M22. The Vendor must have successfully implemented at least three (3) COTS systems comparable to the specifications in this proposal in terms of functionality for other State governments or large metropolitan areas within the United States and must be in full operation for at least three (3) years.

Reporting

M22. Allow for electronic provider reporting, including access for providers to previously reported cases and electronic lab reports from their facilities.

M23. Capability for sending National Electronic Telecommunications System for Surveillance (NETSS) files to CDC for all reportable diseases.

Technical

M24. The EDSS will be a vendor hosted solution commonly referred to as Software as a Service (SaaS) solution.

M25. Replicate the existing I-NEDSS and transfer over all existing data.

M26. Handle volume of current I-NEDSS system (250,000+ records daily). System is scalable to handle ingestion of lab test results volume of 250,000+ per day without affecting the performance of business operations.

M27. Integrate with the geocoder for address validation in real time for all addresses (ELR, electronic case reporting (eCR), and manual entry).

M28. Capability for direct interfacing with the system using Application Programming Interfaces (API) for imports and export of information.

M29. System must have the capability to support >3000 active users and >1000 concurrent users.

M30. Must have the ability for file uploads (e.g. HTML versions of eCR, pdfs, images, etc.) to append to the case record and storage/retrieval of the files on the application database.

Security

M31. Role-based security by program area and jurisdiction.

M32. Support definitions of roles with assigned levels of access, viewing, data entry, editing and auditing.

M33. The solution provided must meet all Department of Innovation and Technology (DoIT) security requirements as defined in Appendix A: Security Requirements.

M34. Log actions by users and allows for auditing of workflow, who logged in, when, what cases were viewed, what was changed within the case**.**

Help Desk, Training and Support

M35. Vendor must staff a dedicated Help Desk specifically for the data system that includes a dedicated email address and phone line. This Help Desk must be available for all system users to contact with issues and technical assistance needs. The Help Desk must be available from 8:00 AM to 5:00 PM CST during the normal work week excluding holidays recognized by the State of Illinois. Vendor must establish and maintain a help desk ticket tracking system to record and manage incident tickets and monitor Service Level Agreement (SLA) goals.

M36. Vendor must provide Hypercare support for six (6) months period of time immediately following a system Go Live where an elevated level of support is available to ensure the seamless adoption of a new system. The main purpose of the Hypercare period is to closely monitor customer service, data Integrity and the smooth operations of the implemented application for perspectives of technical support, on-site availability of the support team, system configuration issues to ensure smooth transition from operational and technical perspective.

M37. Vendor must provide hands-on (onsite and online) training for IDPH Staff to include training materials, for operational and technical staff. Vendor and IDPH must sign-off on operational and technical training**.** The Vendor's Proposal must include a curriculum outline, types of course materials, and a list of objectives and outcomes for the training. The Vendor must agree to provide both onsite and online administrator, new-user, and refresher training course at least annually as long as it hosts the system. Both the Vendor and the Agency must sign off to indicate when any training task is completed.

Deployment

M39. Vendor must have experience with highly complex deployment structures that include multiple phases of introducing capabilities (go-lives). The vendors proposal shall include a proposal based on the State's requirements that completes any proofs of concept and deploys minimum viable product (MVP) with monthly to quarterly releases thereafter for prioritized features not included in the MVP.

Desirable Elements

State's Desirable Elements while not mandatory, are very important to the State. Vendors responding to Desirable specifications will be given points during evaluation of technical responses that correspond to the level of compliance and the quality of the Vendor's proposal. Each substantive response to a Desirable Element should include a detailed description of how the Vendor's solution would provide a solution for the State. Evaluation points will be awarded based on the information provided within the detailed response. Vendors may not provide any pricing details in their substantive responses; vendors must provide pricing details in their Price Proposal only using Attachment A – Budget Template, which will be evaluated separately.

System

D1. Contact tracing capabilities for surveillance of diseases which take into consideration, symptom monitoring, quarantine monitoring, risk/exposure assessments, reporting and analysis of case and contract information for possible outbreaks.

D2. Describe the system's Data Warehouse capabilities for a unified repository used to report and analyze information using a common data model.

D3. Describe the system's capabilities to ingest electronic case reports (eCR) and electronic lab reports. Capability to ingest eCR and map fields to specified module fields and append an HTML file of eCR to be viewable to the user.

D4. Describe the system's capabilities for a Page Builder module for design of data collection forms which allows for on-the-fly modifications for changes to modules and addition of emerging diseases.

D5. Describe the system's capabilities to allow for import of data from other systems, including contact tracing, REDCap and large data cleaning projects.

D6. Describe the system's capabilities to provide Local Health Departments (LHDs) with case management and workflow functionality to support the surveillance and follow-up processes used during public health investigations.

D7. Describe the system's capabilities to allow electronic transfer of cases to other states.

D8. Describe the system's capabilities to allow cases to be deduplicated as part of the process flow.

D9. Describe the system’s capabilities to employ a probabilistic matching scheme for all merges of data and manual name search with algorithms using double meta and soundex.

D10. Describe the system’s capabilities to case auto merge, and autocreation based on a probabilistic matching scheme for all diseases.

D11. Describe the system’s capabilities to unmerge the AutoMerged reports.

D12. Describe the system’s capabilities for automatic detection of duplicates and an automated merge based on comparison of the duplicate records.

D13. Describe the system’s capabilities of mass updates through workflows.

D14. Describe the system’s capabilities of developing disease and users’ level specific workflows for the management of disease investigations and surveillance.

D15. Describe the system’s capabilities to allow a robust user management within the application.

D16. Describe the system’s capabilities to custom business rules to be developed for all disease modules.

D17. Describe the system’s capabilities for automated alerts for diseases and automated process alerts.

D18. Describe the system’s capabilities to jump (hyperlink) to switch to specific fields/pages with errors.

D19. Describe the strategy to provide qualified key resources for project implementation to include but not limited to Project Manager, Business Analyst, Configuration Engineer, Training and System Integration Engineer.

D20. Describe in detail Vendor’s experience and how long Vendor has been developing and supporting software of similar scope.

D21. Provide a high-level project plan for implementation of the project. Staffing and timelines should be included in the plan. Define the timeframes for each implementation activity and requirement to be fulfilled. Identify the major project or service milestones and associated deliverables including the following project plan deliverables:

- Project Plan
- Project Schedule
- Implementation Plan
- Change Management Plan
- Testing Plan and Scripts
- Training Plan

Reporting

D22. Describe Reporting module capabilities to extract data for analysis, visualization, and reporting.

D23. Describe the system’s capabilities for a robust reporting feature for canned and ad hoc reports for both health department and provider-based users.

Technical

D24. Describe the system’s capabilities to ingest negative lab reports, connect those reports to existing cases, and deduplicate negative data to serve as denominator data for calculating testing data.

D25. Describe the system’s capabilities for the reporting functionality of all variables collected must be viewable in the reporting database within 30 seconds from entry in the transactional database and importation of all legacy data into the database.

D26. Describe the system’s capabilities to Integrate with the state's immunization and vital records system for deaths and births, the Adverse Pregnancy Outcomes Reporting System, and the outbreak reporting system.

D27. Describe the system’s capabilities for ingesting nonstandard flat files.

D28. Describe the system’s capabilities to support mass updates through file imports.

D29. Describe the system’s capabilities to support connections to multiple databases: DB2, SQL, and MySQL.

D30. Describe the system’s capabilities to incorporate web services.

Security

D31. Describe the system’s capabilities to support Role-based security by program area and jurisdiction.

D32. Describe the system’s capabilities to support definitions of roles with assigned levels of access, viewing, data entry, editing and auditing.

D33. Describe the system’s capabilities to Log actions by users and allows for auditing of workflow, who logged in, when, what cases were viewed, what was changed within the case.

D34. Describe the system’s capabilities to allow for integration with existing state Active Directory.

D35. Describe the system’s capabilities to allow users to view and edit all cases in their jurisdiction and read-only rights for all cases outside of their jurisdiction for all diseases.

D36. Describe the system’s capabilities to Data Archiving to ensure that historical records are keep for auditing purposes and records are only flagged as deleted (no hard deletes of records are allowed).

D37. Describe the system capabilities to prove Multi-level user permissions (e.g., super user, admin, read only, etc.).

D38. Describe the system’s capabilities allow LHDs to see other jurisdiction’s cases based on disease.

Help Desk, Training and Support

D39. Help Desk - Describe in detail technical and help desk support for information technology personnel and end users support. Include availability of assistance through multiple channels including telephone, on-line chat, on-line forms, and email. Indicate average response times including statistics such as mean, standard deviation, median, and inter-quartile range.

D40. Help Desk - Describe the availability of records of help desk activities and the ability to provide a monthly report. In addition, the Vendor should describe the capability to provide access to the system(s) that support help desk operations, or equivalent information, to Agency designated representatives upon request.

D41. Training - Provide a detailed explanation of the training plan for all modules. The plan should include general approach, curriculum outlines, types of course materials, and a list of objectives and outcomes for each type of training.

D42. Training Describe how web-based, online training tutorial (not live) for end users of the system works and can be modified by the State.

D43. Support - Describe Vendor's 24/7/365 emergency technical support escalation policy process. Include the response times, communication methods and escalation procedures that would take effect in the event of a system failure during non-business hours.

D44. Hypercare Technical Support - Describe the Hypercare Technical Support service including but not limited to the following:

- Resolving technical queries of the end user working on the application.
- Bugs and fixes.
- Stabilize and work efficiently in the new IT environment.
- Data integration with various other existing systems.

D45. Hypercare On-site Availability Support - Describe the support service for Hypercare "On-site Availability" support services including but not limited to the following:

- End user queries can be resolved on the spot.
- Floor training for the end users which helps them get a complete understanding of the application which considerably reduces the number of queries hitting the support desk during on- going support.
- Quick adoption of system/modules and staff completely familiar with the application.

D46. Hypercare Handling Configuration Issues and Queries – Describe the support service for Hypercare "Configuration Issues" support services including but not limited to the following:

- Configuration of fields, adding drop down values, modifying field names, changing locations of the fields etc.
- System integration modifications.
- Reporting and Queries.

D47. Hypercare Ensuring Smooth Handover Transition - Describe the support activities for Hypercare "Ensuring smooth handover" Support Services including but not limited to the following:

- Documentation.
- Confirmation from the end users on various processes configured in the application.
- Application's administrator rights to the support team.
- Confirmation on resolution of major issues are reported during this phase.

Deployment

D48. Describe vendor's experience in prioritizing features and requirements, providing joint effort proofs of concept, and providing multi-phase go-lives.

D49. Describe a recommendation for the State that has both six and twelve-month minimum viable product (MVP) deployments with monthly to quarterly releases thereafter for prioritized features not included in earlier deployments.

D50. Describe change management practices for both internal and external users and the IT functions.

Appendix A – Security Requirements

A1. Vendor will notify the State's Chief Information Security Officer within 24 hours of any information breach or other security incident which impacts the State's data.

A2. Vendor must prove compliance with the State of Illinois Vendor Security Controls, based on the current revision of NIST 800-53 security controls for a moderate system, Appendix B: Security Controls.

A3. Vendor shall ensure encryption of State of Illinois data at rest and in motion. This encryption must comply with encryption security controls as defined in the most current version of FIPS 140 using AES encryption with a minimum key length of 256 bits. Vendor must provide a copy of the encryption certificate.

A4. Vendor shall only use State or Participant data, or State-related or Participant-related data for the purposes stated in this Contract.

A5. Vendor shall not use State or Participant data, or State-related or Participant-related data, for any other purpose, including, but not limited to, data mining or bids on other government contracts.

A6. Vendor and/or its agents shall not resell nor otherwise redistribute information gained from its access to the State or Participants.

A7. Vendor shall not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the State.

A8. Vendor shall have a documented security incident policy and plan.

A9. Vendor must maintain a robust and reliable data backup system. Vendor must supply a description of backup methodology and this methodology must meet DOIT's defined MTD and RPO requirements. Vendor must provide proof of backup monitoring and testing at DOIT's request.

A10. Vendor must provide a disaster recovery methodology and provide proof of annual disaster recovery testing, including issues discovered and remediation plans for the issues discovered.

A11. Vendor shall ensure all of data pertinent to this contract remains located within the contiguous United States.

A12. Vendor shall ensure that production data is not used outside of the production environment.

A13. Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State with System Operation Controls report (SOC 2) annually and applicable or Bridge/Gap letter.

A14. Vendor certifies it has undertaken independent third-party audit Statement on Standards for Attestation Engagements (SSAE-18) certifications and must provide the State with System Operation Controls report (SOC 1) annually and applicable or Bridge/Gap letter.

A15. Security Control Assessment – In the event that a SOC report and Bridge/Gap letter cannot be supplied, the Vendor must perform an internal security control assessment based on the State of Illinois Security Controls for Vendors

The results of this assessment will be documented in a Security Assessment Report (SAR) to be approved by the State. Plan of Action and Milestones (POA&M): After DoIT reviews and approves the SOC or SAR, the Vendor shall develop a POA&M. The POA&M should be a living document that is based on the findings and recommendations of the SAR. The POA&M should describe the deficiencies in the security controls, address the residual risk and detail plans for remediation. Vendor will provide the State with the POA&M and monthly updates regarding progress toward remediation of identified deficiencies in security controls.

A16. Vendor must provide a copy of all data to the State without delay upon request by the State.

A17. Vendor must provide a copy of all data to the State in a format determined by the State prior to termination of contract.

A18. Data Destruction: After transfer of data back to DoIT and/or migration of data to a new or replacement system, and following verification of the data, Vendor must sanitize all media that contained State of Illinois data. Vendor must use the current revision of NIST Special Publication 800-88; Guidelines for Media Sanitization. Vendor must provide certification of media sanitization including the method, date and time.

A19. The State of Illinois is required to comply with the below laws, standards and regulations. Vendors must ensure compliance with the below as appropriate based upon the formal risk assessment to include a data classification and system categorization process.

1. Illinois Identity Protection Act (5 ILCS 179)
2. Illinois Personal Information Protection Act (815 ILCS 530)
3. Federal Centers for Medicare & Medicaid Services (CMS) MARS-E Document Suite, Version 2.0 Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges – current version.
4. Federal Centers for Medicare & Medicaid Services Information Security Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements – current version.

A20. Vendor must perform Penetration testing at regular intervals according to Cloud Security Alliance (CSA) and Open Web Application Security Project (OWASP) recommendations.

A21. Vendor must allow the State of Illinois Technical Safeguards Unit the ability to perform vulnerability scans at initial implementation and when there are major modifications to the application as defined in the Vulnerability Scanning Agreement.

A22. DoIT may with reasonable notice to Vendor, conduct a security assessment of Vendor's solution which may include the following:

I. Prior to initial "Official" production roll out of the application:
   - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application.
   - Manual verification of scan results with the same credentials
   - Manual testing of the application for vulnerabilities
   - DoIT will not conduct any Denial of Service (DOS) attacks
   - DoIT will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

II. On a quarterly basis for the for the first year after initial production deployment;
   - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application.
   - Manual verification of scan results with the same credentials
   - Manual testing of the application for vulnerabilities
   - DoIT will not conduct any DOS attacks
   - DoIT will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

III. Prior to any enhancements or upgrades being deployed to production after the initial "official" production roll out of the application,
   - Whitelisted scanning and manual testing of the application only, with application credentials equal to the least privileged role within the application.
   - Manual verification of scan results with the same credentials
   - Manual testing of the application for vulnerabilities
   - DoIT will not conduct any DOS attacks
   - DoIT will not scan or test any infrastructure devices (servers, switches, routers, intrusion protection system, firewalls, etc.)

IV. Monthly vulnerability scan – no whitelisting, non-credentialed scan (same day every month).
   - Vendor is required to notify hosting provider that DoiT will be scanning but does not need any whitelisting

V. Remediation of high vulnerabilities and medium vulnerabilities within the application detected during the security assessments that are determined by the SOI to pose an unacceptable risk, must be remediated by the vendor. Rescans to verify remediation prior to deployment to the production will be conducted by DoiT at its own expense.

Appendix B – Security Controls

NIST 800-53 v4 – Security and Privacy Controls

Access and Control (AC)

Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

AC Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #’s
• Access Control Policy and Procedures	AC-1	
• Account Management	AC-2	(1), (2), (3), (4)
• Access Enforcement	AC-3	
• Information Flow Enforcement	AC-4	
• Separation of Duties	AC-5	
• Least Privilege	AC-6	(1), (2), (5), (9), (10)
• Unsuccessful Logon Attempts	AC-7	
• System Use Notification	AC-8	
• Session Lock	AC-11	(1)
• Session Termination	AC-12	
• Permitted Actions without Identification or Authentication	AC-14	
• Remote Access	AC-17	(1), (2), (3), (4)
• Wireless Access	AC-18	(1)
• Access Control for Mobile Devices	AC-19	(5)
• Use of External Information Systems	AC-20	(1), (2)
• Information Sharing	AC-21	
• Publicly Accessible Content	AC-22	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Awareness and Training (AT)

Organizations must (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

AT - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Security Awareness and Training Policy and Procedures	AT-1	
• Security Awareness Training	AT-2	(2)
• Role-Based Security Training	AT-3	
• Security Training Records	AT-4	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Audit and Accountability (AU)

Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users, so they can be held accountable for their actions.

AU - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Audit and Accountability Policy and Procedure	AU-1	
• Audit Events	AU-2	(3)
• Content of Audit Records	AU-3	(1)

• Audit Storage Capacity	AU-4	
• Response to Audit Processing Failures	AU-5	
• Audit Review, Analysis, and Reporting	AU-6	(1), (3)
• Audit Reduction and Report Generation	AU-7	(1)
• Time Stamps	AU-8	(1)
• Protection of Audit Information	AU-9	(4)
• Audit Record Retention	AU-11	
• Audit Generation	AU-12	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Certification, Accreditation, and Security Assessments (CA)

Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organization information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Security Assessment and Authorization Policy and Procedures	CA-1	
• Security Assessments	CA-2	(1)
• System Interconnections	CA-3	(5)
• Plan of Action and Milestones	CA-5	
• Security Authorization	CA-6	
• Continuous Monitoring	CA-7	(1)
• Internal System Connections	CA-9	

Authority	
NIST	SP 800-53 Security and Privacy Controls
NIST	SP 800-53A Assessing Security Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Configuration Management (CM)

Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

<u>CM - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):</u>

Security Control Summary	Control #	Enhancement #'s
• Configuration Management Policy and Procedures	CM-1	
• Baseline Configuration	CM-2	(1), (3), (7)
• Configuration Change Control	CM-3	(2)
• Security Impact Analysis	CM-4	
• Access Restrictions for Change	CM-5	
• Configuration Settings	CM-6	
• Least Functionality	CM-7	(1), (2), (4)
• Information System Component Inventory	CM-8	(1), (3), (5)
• Configuration Management Plan	CM-9	
• Software Usage Restrictions	CM-10	
• User-Installed Software	CM-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Contingency Planning (CP)

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

CP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Contingency Planning Policy and Procedures	CP-1	
• Contingency Plan	CP-2	(1), (3), (8)
• Contingency Training	CP-3	
• Contingency Plan Testing	CP-4	(1)
• Alternate Storage Site	CP-6	(1), (3)
• Alternate Processing Site	CP-7	(1), (2), (3)
• Telecommunications Services	CP-8	(1), (2)
• Information System Backup	CP-9	(1)
• Information System Recovery and Reconstitution	CP-10	(2)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organizational information systems.

IA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• Identification and Authentication Policy and Procedures	IA-1	
• Identification and Authentication (Organizational Users)	IA-2	(1), (2), (3), (8), (11), (12)

• Device Identification and Authentication	IA-3	
• Identifier Management	IA-4	
• Authentication Management	IA-5	(1), (2), (3), (11)
• Authenticator Feedback	IA-6	
• Cryptographic Module Authentication	IA-7	
• Identification and Authentication (Non-Organizational Users)	IA-8	(1), (2), (3), (4)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Incident Response (IR)

Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and or authorities.

<u>IR - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):</u>

Security Control Summary	**Control #**	**Enhancement #'s**
• Incident Response Policy and Procedures	IR-1	
• Incident Response Training	IR-2	
• Incident Response Testing	IR-3	(2)
• Incident Handling	IR-4	(1)
• Incident Monitoring	IR-5	
• Incident Reporting	IR-6	(1)
• Incident Response Assistance	IR-7	(1)
• Incident Response Plan	IR-8	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines

IDoIT	IDoIT Policies and Associated Standards and Guidelines

Maintenance (MA)

Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

<u>MA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):</u>

Security Control Summary	**Control #**	**Enhancement #'s**
• System Maintenance Policy and Procedures	MA-1	
• Controlled Maintenance	MA-2	
• Maintenance Tools	MA-3	(1), (2)
• Nonlocal Maintenance	MA-4	(2)
• Maintenance Personnel	MA-5	
• Timely Maintenance	MA-6	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Media Protection (MP)

Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

<u>MP - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):</u>

Security Control Summary	**Control #**	**Enhancement #'s**
• Media Protection Policy and Procedures	MP-1	
• Media Access	MP-2	
• Media Marking	MP-3	
• Media Storage	MP-4	

• Media Transport	MP-5	(4)
• Media Sanitization	MP-6	
• Media Use	MP-7	(1)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Physical and Environmental Protection (PE)

Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

<u>PE - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):</u>

Security Control Summary	Control #	Enhancement #’s
• Physical and Environmental Protection Policy and Procedures	PE-1	
• Physical Access Authorizations	PE-2	
• Physical Access Control	PE-3	
• Access Control for Transmission Medium	PE-4	
• Access Control for Output Devices	PE-5	
• Monitoring Physical Access	PE-6	(1)
• Visitor Access Records	PE-8	
• Power Equipment and Cabling	PE-9	
• Emergency Shutoff	PE-10	
• Emergency Power	PE-11	
• Emergency Lighting	PE-12	
• Fire Protection	PE-13	(3)
• Temperature and Humidity Controls	PE-14	
• Water Damage Protection	PE-15	
• Delivery and Removal	PE-16	
• Alternate Work Site	PE-17	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Planning (PL)

Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individual's accessing the information systems.

PL - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Security Planning Policy and Procedures	PL-1	
• System Security Plan	PL-2	(3)
• Rules of Behavior	PL-4	(1)
• Information Security Architecture	PL-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Personnel Security (PS)

Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information system are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

PS - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**

• Personnel Security Policy and Procedures	PS-1	
• Position Risk Designation	PS-2	
• Personnel Screening	PS-3	
• Personnel Termination	PS-4	
• Personnel Transfer	PS-5	
• Access Agreements	PS-6	
• Third-Party Personnel Security	PS-7	
• Personnel Sanctions	PS-8	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

RA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	**Control #**	**Enhancement #'s**
• Risk Assessment Policy and Procedures	RA-1	
• Security Categorization	RA-2	
• Risk Assessment	RA-3	
• Vulnerability Scanning	RA-5	(1), (2), (5)

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

System and Services Acquisition (SA)

Organizations must: (i) allocate sufficient resources to adequately protect organizations information system; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and or services outsourced from the organization.

SA - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Services Acquisition Policy and Procedures	SA-1	
• Allocation of Resources	SA-2	
• System Development Life Cycle	SA-3	
• Acquisition Process	SA-4	(1), (2), (9), (10)
• Information System Documentation	SA-5	
• Security Engineering Principles	SA-8	
• External Information System Services	SA-9	(2)
• Developer Configuration Management	SA-10	
• Developer Security Testing and Evaluation	SA-11	

Authority	
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

System and Communications Protection (SC)

Organizations must: (i) monitor, control, and protect organizational communications (i.e. information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries for the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organization information systems.

SC - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #’s
• System and Communication Protection Policy and Procedures	SC-1	
• Application Partitioning	SC-2	
• Information in Shared Resources	SC-4	
• Denial of Service Protection	SC-5	
• Boundary Protection	SC-7	(3), (4), (5), (7)
• Transmission Confidentiality and Integrity	SC-8	(1)
• Network Disconnect	SC-10	
• Cryptographic Key Establishment and Management	SC-12	
• Cryptographic Protection	SC-13	
• Collaborative Computing Devices	SC-15	
• Public Key Infrastructure Certificates	SC-17	
• Mobile Code	SC-18	
• Voice Over Internet Protocol	SC-19	
• Secure Name/Address Resolution Service (Authoritative Source)	SC-20	
• Secure Name/Address Resolution Service (Recursive or Caching Resolver)	SC-21	
• Architecture and Provisioning for Name/Address Resolution Service	SC-22	
• Session Authenticity	SC-23	
• Protection of Information at Rest	SC-28	
• Process Isolation	SC-39	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines

System and Information Integrity (SI)

Organizations must: (i) identify, report, and correct information and information systems flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems, and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

SI - NIST Security Controls and Control Enhancements (for Moderate Security Categorization):

Security Control Summary	Control #	Enhancement #'s
• System and Information Integrity Policy and Procedures	SI-1	
• Flaw Remediation	SI-2	(2)
• Malicious Code Protection	SI-3	(1), (2)
• Information System Monitoring	SI-4	(2), (4), (5)
• Security Alerts, Advisories and Directives	SI-5	
• Software, Firmware, and Information Integrity	SI-7	(1), (7)
• Spam Protection	SI-8	(1), (2)
• Information Input Validation	SI-10	
• Error Handling	SI-11	
• Information Handling and Retention	SI-12	
• Memory Protection	SI-16	

Authority	
CFR	HIPAA 45 CFR - 160, 162, 164
NIST	SP 800-53 Security and Privacy Controls
FIPS	200 Minimum Security Controls
IRS	1075 Tax Information Security Guidelines
IDoIT	IDoIT Policies and Associated Standards and Guidelines